

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED
AUSTIN DIVISION
2004 NOV -3 PM 1:21
U.S. DISTRICT COURT
AUSTIN, TEXAS
BY: *102*

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTOPHER ANDREW PHILLIPS,

Defendant.

) CRIMINAL NO. A-04-CR-
) **A04 CR 247 LY**
)
) INDICTMENT
) Violation:
) Count 1: 18 USC 1030(a)(5)(A)
) (Fraud and Related Activity in
) Connection with Computers);
) Counts 2 and 3: 18 USC 1029(a)(3)
) (Fraud and Related Activities
) in Connection with Access Devices);
) Count 4: 18 USC 1028(a)(6)
) (Fraud and Related Activity in
) Connection with Identification
) Documents, Authentication Features, and
) Information)

THE GRAND JURY CHARGES THAT:

COUNT 1
[18 U.S.C. 1030(a)(5)(A)(ii), (B)(i)]

Introduction

1. On or about Fall Semester, 2001, through on or about Spring Semester, 2003, **Defendant, CHRISTOPHER ANDREW PHILLIPS**, was a Computer Science major at the University of Texas at Austin (hereinafter UT).
2. On or about January 30, 2002, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, attempted to breach the security of hundreds of outside computer systems and was detected by the ITS Information Security Office at UT. The ITS Information Security Office at UT warned the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, not to further attempt to

breach the security of these outside computer systems.

3. On or about February 15, 2002, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, attempted to breach the security of hundreds of outside computer systems and was detected by the ITS Information Security Office at UT. The ITS Information Security Office at UT warned the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, not to further attempt to breach the security of these outside computer systems.

4. On or about April 8, 2002, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, was again detected by the ITS Information Security Office at UT while trying to breach the security of hundreds of outside computer systems. The ITS Information Security Office at UT again warned the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, not to further attempt to breach the security of these outside computer systems.

5. From on or about October 2002, to on or about November 2002, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, downloaded biographical data from an Internet Web site providing genealogical information of individuals born during the years 1940 to 1984 including name, date of birth, gender, father's name, mother's maiden name, and county of birth for the following Texas counties: Bexar, Collin, Dallas, Denton, El Paso, Fort Bend, Harris, Hidalgo, Tarrant and Travis.

6. On or about January 30, 2003, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, created a computer program to breach the security of, or "hack into," a protected UT computer system used for interstate and foreign commerce and communication and for which the **Defendant** did not have access in order to discover the names and social security numbers of individuals in the UT computer system via the TXCLASS web site.

7. The **Defendant, CHRISTOPHER ANDREW PHILLIPS**, had no authorization to access the TXCLASS system.

8. From on or about January 29, 2003, to on or about March 2, 2003, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, used the computer program he created to breach the security of, or “hack into,” this protected UT computer system via the TXCLASS web site for which he did not have access and stole over 37,000 names and social security numbers of individuals in the UT system.

9. By “hacking” into this protected UT computer system and running the program to steal the names and social security numbers of individuals in the UT computer system via the TXCLASS web site, the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, overloaded the UT computer system and caused massive failures that shut down the TXCLASS computer system on three occasions on February 26, 27, and 28, 2003. By the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, overloading and damaging the TXCLASS computer system with his “hacking” program, other UT computer programs related to interstate and foreign communication and commerce became inaccessible and unusable as well including all web-based services and all services requiring mainframe identification authentication, such as admission application submissions, tuition payments, and course registration.

10. Due to the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, breaching the security of, or “hacking into,” this protected UT computer system, UT suffered losses of approximately \$122,000, including the cost of responding to the offense and conducting damage assessments, and another \$45,000 in losses incurred by UT to warn individuals whose names and social security numbers were stolen by the **Defendant** about potential identity theft.

11. The **Defendant, CHRISTOPHER ANDREW PHILLIPS**, also possessed on his computer with intent to defraud more than 15 credit card, bank account, financial aid information, and Social Security numbers, of multiple individuals who did not give the **Defendant, CHRISTOPHER ANDREW PHILLIPS**, permission to have such information.

12. "TXCLASS" is a web-based service for tracking the training classes that UT employees attend. The system was intended to be used by UT employees to view a list of classes he/she attended, or by UT supervisors to review a list of classes for one or more employees. The database is accessed by using the social security number (SSN) of the authorized person(s) whose training record is to be inspected. Only employees and supervisors were intended to be authorized to use the system. As UT subsequently learned, however, access to TXCLASS also resulted in access through the unified database to a broader range of information than employee class attendance records, including names, tuition payments, class registration, admission applications, job titles, campus addresses and phone numbers, and/or e-mail addresses from the centralized UT database of Electronic Identifier (EID) information pertaining to faculty, staff, students, former students, and others.

13. The "Internet" is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, the individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet.

14. "Internet Service Providers" ("ISPs") provide individuals and businesses with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers'

behalf; and, may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information (including source and destination e-mail and/or Internet Protocol addresses), posting information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a “remote computing service.”

15. A “server” is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called “clients.” In a large company, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client’s computer via the network. Notably, server computers can be physically stored in any location: it is common for a network’s server to be located hundreds (and even thousands) of

miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a “web server.” An e-mail server allows users to post and read messages, and to communicate via private electronic mail. An “IRC” (Internet Relay Chat) server allows users to engage in “chat sessions,” which are real-time conversations where the participants communicate by using their keyboards, to send and receive files, and to share information. Using a telephone or other telecommunications line, one can transmit and receive e-mail or IRC chats between computers.

16. The “Internet Protocol address” (or simply “IP” address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

17. When an ISP or other provider uses “dynamic IP addresses,” the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer’s computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer’s IP address normally differs each time he dials into the ISP. As such, a specific date and time is usually necessary to identify a particular user assigned to a particular IP address.

18. A “static IP address” is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.

19. Via a telephone or other telecommunications line, a computer user can transport a computer file to his own computer, so that the computer file is stored in his computer. The process of transporting a file to one’s own computer is called “downloading.” The user can then view the file on his/her computer screen (monitor), and can “save” or retain the file on his/her computer for an indefinite time period. In addition to permanently storing the file on the computer, the user may print the file. The original file that was downloaded is also maintained in the originating computer.

20. Via a telephone or other telecommunications line, a computer user can send a file from the computer to another individual on the Internet. This process of sending a file is called “uploading.” The process of “uploading” is similar to the “downloading” process except the user is sending the computer file to others instead of retrieving the information from another computer.

Charge

From on or about January 29, 2003, to on or about March 4, 2003, in the Western District of Texas, and elsewhere, the **Defendant**,

CHRISTOPHER ANDREW PHILLIPS,

intentionally accessed a protected computer without authorization and recklessly caused damage to a protected computer, to wit: causing massive failures that shut down the TXCLASS computer system on three occasions, which also made other UT computer programs also related to interstate and foreign communication and commerce became inaccessible and unusable as

well, including all web-based services and all services requiring mainframe identification authentication, such as admission application submissions, tuition payments, and course registration, thereby creating a loss to more than one person during a 1-year period aggregating at least \$5,000 in value, to wit: a loss of \$122,000 to UT.

In violation of Title 18, United States Code, Section 1030(a)(5)(A)(ii), (B)(i).

COUNT 2
[18 U.S.C. 1029(a)(3)]

The Introduction of Count 1 is incorporated by references as if fully set forth.

From on or about January 29, 2003, to on or about March 5, 2003, in the Western District of Texas, and elsewhere, the **Defendant**,

CHRISTOPHER ANDREW PHILLIPS,

knowingly and with the intent to defraud possessed fifteen or more unauthorized access devices, to wit: 37,000 Social Security numbers stolen from the University of Texas at Austin's computers.

In violation of Title 18, United States Code, Section 1029(a)(3).

COUNT 3
[18 U.S.C. 1029(a)(3)]

The Introduction of Count 1 is incorporated by references as if fully set forth.

On or about March 5, 2003, in the Western District of Texas, and elsewhere, the

Defendant,

CHRISTOPHER ANDREW PHILLIPS,

knowingly and with the intent to defraud possessed fifteen or more unauthorized access devices, to wit: credit card, bank account, and/or Social Security numbers belonging to multiple people.

In violation of Title 18, United States Code, Section 1029(a)(3).

COUNT 4
[18 U.S.C. 1028(a)(6)]

The Introduction of Count 1 is incorporated by references as if fully set forth.


From on or about January 29, 2003, to on or about March 5, 2003, in the Western District of Texas, and elsewhere, the **Defendant,**

CHRISTOPHER ANDREW PHILLIPS,

knowingly possessed an identification document and an authentication feature of the United States, to wit: 37,000 Social Security numbers, which all were stolen knowing that such document and authentication feature were stolen.

In violation of Title 18, United States Code, Section 1028(a)(6).

A TRUE BILL.



FOREPERSON OF THE GRAND JURY

JOHNNY SUTTON
United States Attorney

By: 

MARK T. ROOMBERG
Assistant United States Attorney